ISSN 2282-6343

Centro Studi Internazionali

Evoluzione del quadro di sicurezza cibernetica nazionale in prospettiva futura

di Francesco Tosato e Michele Taufer

APRILE 2016

INDICE

INTRODUZIONE

La nostra società, le nostre economie e anche le minacce che pervadono il nostro mondo sono sempre più caratterizzate dalla dimensione cibernetica. L'avvento dell'Information Technology (IT) e successivamente di internet ha permesso di aumentare in maniera sensibile e per certi versi rivoluzionaria lo scambio dei dati e delle informazioni su scala globale.

Conseguentemente, il settore che ha beneficiato maggiormente di questa evoluzione tecnologica è stato quello economico, specie se si considera il fatto che la quasi totalità delle economie mondiali fa perno su sistemi di libero scambio che si basano sulla libera circolazione di beni, servizi e conoscenze. Una simile mole di informazioni sensibili, costantemente in transito nel web, apre la porta a nuove minacce, soprattutto derivanti da coloro che, Stati o gruppi di individui, sono intenzionati ad appropriarsene per poi utilizzarli a discapito dei legittimi proprietari.

In particolare, il nostro Paese è caratterizzato da una delle principali economie a livello mondiale: una peculiarità, dovuta sia al volume degli scambi economici sia al know how posseduto in alcuni settori specifici. L'Italia costituisce quindi uno dei principali obbiettivi per quanto concerne gli attacchi di tipo informatico subiti come dimostrato dal nono posto nel ranking mondiale della Kaspersky Lab. Questa circostanza si spiega chiaramente dato l'interesse di molte economie emergenti a sottrarre parte del know how tecnologico e industriale italiano in un'ottica di competizione a livello globale.

Se l'economia è uno dei settori che ha risentito maggiormente della rivoluzione informatica e dell'avvento di internet, anche quello dei conflitti armati ne è stato profondamente permeato e mutato. Nati come mezzi di supporto e di comunicazione militare, l'informatica e internet, con l'avvento della Revolution in Military Affairs (RMA) statunitense degli anni Novanta, hanno definitivamente mostrato agli occhi del mondo il livello di letalità e di efficacia raggiunto dal potere militare americano, altamente informatizzato, netcentrico e razionale nell'opera di targeting, specie nei confronti di Forze Armate nemiche ancora ancorate al concetto di massa d'urto, quale perno e parametro di riferimento del potere militare di uno Stato.

In tempi recenti, poi, la sempre maggiore integrazione tra mezzi militari di tipo classico (Legacy) e le tecnologie informatiche ha permesso la nascita di quella che è la dimensione cyber dei conflitti, un "ambiente operativo" da utilizzare e da cui partire per condurre veri e propri attacchi, con ripercussioni fisiche ai danni di sistemi e infrastrutture nemiche, in tutto e per tutto identici agli effetti degli attacchi cinetici di tipo classico.

La dimensione cyber è ed evolverà sempre più in futuro, andando a costituire così, a tutti gli effetti, la quinta dimensione dei

moderni conflitti armati. Ecco pertanto che i principali Paesi a livello mondiale stanno dedicando sempre più risorse, sia umane che economiche, per lo sviluppo di adeguate dottrine e procedure da impiegare in maniera efficace nelle operazioni militari da svolgere all'interno dell'ambiente cyber allo scopo di aumentare le capacità di difesa e anche quelle di deterrenza.

IL QUADRO INTERNAZIONALE

Sulla base di quanto introdotto, seguirà ora una breve disamina di come i principali Paesi europei e gli Stati Uniti d'America stanno affrontando i mutamenti e gli scenari operativi legati all'ambiente cyber e alle minacce che da quest'ultimo ne derivano.

Regno Unito

Nel Regno Unito il dominio SIGINT e cyber è presidiato dall'agenzia Goverment Communication Headquarters (GCHQ). Questa realtà si occupa di tutte le dinamiche afferenti la cybersecurity e la cyberintelligence a beneficio sia delle istituzioni britanniche sia delle Forze Armate. Il GCHQ è un vero e proprio servizio, al pari dell'MI6 (Intelligence) e dell'MI5 (Sicurezza Interna), ed è sotto il formale controllo del Joint Intelligence Committee (JIC). Il GCHQ svolge, però, anche un importante ruolo di supporto alle Forze Armate in quanto collabora con esse alla costruzione di un ambiente di comunicazione cyber più sicuro e si occupa della protezione delle industrie operanti per la Difesa. A dimostrazione di quanto siano stretti i rapporti, nella sede principale dell'agenzia è ospitata una cellula militare, la Joint Cyber Unit, con il compito di sviluppare nuove tattiche e dottrine al fine di svolgere operazioni nel cyberspazio. Oltre ad operare a sostegno della Difesa, il GCHQ è anche, attraverso l'unità CESG, l'autorità tecnica nazionale per la sicurezza informatica della Gran Bretagna ed è, quindi, l'entità che si occupa anche di verificare e aggiornare la resilienza dell'infrastruttura cyber britannica, la capacità dello Stato di comunicare in maniera sicura con i propri cittadini e la protezione delle informazioni sensibili per la sovranità britannica. Infine, l'agenzia, dispone anche di capacità di attacco cyber che dovrebbero essere in gran parte concentrate nell'unità denominata Joint Threat Research Intelligence Group. Si dovrebbe trattare solo di capacità offensive funzionali all'attività operativa di intelligence e non di cyberweapons che, invece, rimangono di competenza delle Forze Armate.

Francia

In Francia il comparto SIGINT è primariamente presidiato dalla Direction Générale de la Sécurité Extérieure (DGSE), il servizio di intelligence francese per la sicurezza esterna dipendente dal Ministero della Difesa. La DGSE, in quanto dipendente

dalla Difesa e titolare anche delle operazioni coperte, sembra essere, al momento, anche l'unica entità francese in grado di condurre operazioni cyber di tipo offensivo a livello strategico. Per quanto riguarda, invece, le capacità di cybersecurity e cyberdefence, Parigi nel Libro Bianco 2008 e, ancor di più, nell'edizione 2013 ha definito il dominio cyber come fondamentale per il sostegno dell'autonomia politica e strategica del Paese mentre il successivo patto "Difesa Cyber 2016" ha individuato 50 azioni pratiche da mettere in atto nel biennio 2014-2016.

Di conseguenza, le capacità di difesa e resilienza cyber del Paese sono state ampliate in maniera notevole con la creazione dell'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), sottoposta al Segretariato Generale della Difesa e della Sicurezza Nazionale dipendente direttamente dal Primo Ministro. L'ANSSI è l'autorità nazionale per la sicurezza e la difesa dei sistemi informatici ed ha il compito di individuare contenere e rispondere ad attacchi cibernetici sviluppando in maniera costante le dottrine operative in tale ambito. Attualmente dispone di 500 agenti che saranno aumentati a 600 entro la fine del 2016. Le competenze dell'ANSSI comprendono tutta la sfera dell'infrastruttura civile e quella statale francese ad eccezione delle Forze Armate.

Infatti, per le reti militari la responsabilità ricade sotto la Direzione Generale degli Armamenti (DGA) che dispone di un apposito comando cyber (COCYBER). Anche se si tratta di due strutture distinte, la collaborazione è totale e, infatti, il Centro di Analisi per la Lotta Informatica Difensiva (CALID) delle Forze Armate è localizzato in Bretagna nella medesima struttura che ospita anche l'omologa realtà civile a guida ANSSI. Nel complesso, la soluzione francese appare meno interforze di quella britannica e prevede una struttura militare difensiva (COCYBER), una civile (ANSSI), una per il contrasto al cybercrime afferente al Ministero dell'Interno e una per attività offensive in capo alla DGSE.

Germania

La Germania predisporrà entro il 2016 un nuovo Libro Bianco della Difesa che, dalle prime anticipazioni, sarà concentrato sul contrasto della minaccia rappresentata dalla "guerra ibrida" e che conterrà anche una nuova strategia relativa al dominio cyber. In questo settore appare ormai evidente che Berlino sia orientata a rivoluzionare il quadro attuale, che vede le competenze cyber disperse in più entità, attraverso la creazione di un'apposita agenzia di cybersecurity, mentre verranno sviluppate anche capacità attive (ovvero offensive) che, però, resteranno di esclusiva competenza delle Forze Armate in modo da essere sottoposte

a tutti i controlli parlamentari e costituzionali del caso.

Se questo è il probabile prossimo futuro, attualmente la struttura di cybersecurity e cyberdefence è ancora strutturata seguendo le tradizionali competenze ministeriali. Di conseguenza, le operazioni SIGINT e cyber estere rientrano nelle competenze del Bundesnachrichtendienst (BND), il servizio di intelligence per l'esterno della Repubblica Federale tedesca direttamente dipendente dall'Ufficio del Cancelliere. Di contro, la protezione cibernetica dell'infrastruttura statale e nazionale tedesca è demandata al Bundesamt für Sicherheit in der Informationstechnik (BSI – Ufficio Federale per la Sicurezza Informatica) dipendente dal Ministero dell'Interno. Il BSI è l'autorità nazionale per la cybersecurity e ha il compito di promuovere la sicurezza informatica sia a livello istituzionale sia a favore delle imprese private. Ad affiancare questa realtà vi è, poi, la rete dei vari computer emergency response teams (CERTs) e il Bundesamt für Verfassungsschutz (BfV- Ufficio Federale per la Protezione della Costituzione) ovvero il servizio di sicurezza interna tedesco.

Le capacità operative in ambito offensivo, come già accennato, sono in corso di sviluppo da parte delle Forze Armate tedesche. La struttura di riferimento è Kommando Strategische Aufklärung (KSA - Comando di Ricognizione Strategica). Questa realtà sovraintende un'apposita unità, il Dipartimento di Informatica e Computer Network Operations, che si occupa proprio di sviluppare e condurre le operazioni cyber attive di tipo militare. Entro il 1° aprile 2017, però, tutte le funzioni saranno accentrate in una nuova struttura interforze con quartier generale a Bonn che sovraintenderà le operazioni cyber, l'infrastruttura IT, le comunicazioni militari e operative e i servizi di geolocalizzazione. E' previsto che la nuova realtà potrà contare su investimenti di poco superiori al miliardo di euro e che raggiunga la piena operatività nel 2021.

Stati Uniti

Sin dall'inizio della Presidenza Obama, il tema della cybersecurity, della difesa dagli attacchi cibernetici e della deterrenza del Paese in quest'ambito hanno costituito una delle priorità della Casa Bianca, come ben rappresentato dalla pubblicazione della International Strategy For Cyberspace nel 2011. L'argomento è stato, poi, ulteriormente sviluppato attraverso la presentazione del Cybersecurity National Action Plan lo scorso febbraio che ha individuato 4 assi di intervento per adeguare alle nuove minacce la struttura cibernetica statunitense: istituzione del Chief Information Security Officer[1], incremento della collaborazione tra governo e aziende strategiche, rafforzamento della partnership pubblico-privato soprattutto in supporto alle

1 Chief Information Security Officer: si occuperà di coordinare gli sforzi in materia di cybersecurity delle agenzie federali americane.

PMI, rafforzamento della protezione delle infrastrutture critiche. Data la complessità della sfida da affrontare, lo sforzo messo in campo da Washington coinvolge un numero rilevante di enti e agenzie governative. Al fine di comprendere meglio la postura statunitense, quindi, risulta agevole suddividere i compiti tra operazioni interne ed esterne, limitando l'elenco alle agenzie di vertice che coordinano l'intero sforzo nazionale in materia cyber.

La difesa degli assetti chiave in ambito civile, così come la protezione delle attività economiche, ricadono sotto il controllo del Department of Homeland Security (DHS) in concorso con la National Security Agency (NSA) per quanto concerne le operazioni di Information Assurance. Il DHS è l'autorità nazionale con il compito della protezione delle infrastrutture critiche grazie anche all'impiego del National Cybersecurity and Communications Integration Center (NCCIC) che a sua volta può fare perno sull'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) al fine di ridurre i rischi dei settori dell'economia e delle strutture nazionali più esposte alla minaccia cibernetica. Le strutture militari vengono invece protette dallo US Cyber Command (USCYBERCOM), un comando interforze attualmente subordinato allo US Strategic Command (USSTRATCOM). Sempre allo USCYBERCOM spettano anche le azioni cibernetiche da condurre verso l'esterno, tra cui rivestono particolare importanza le Offensive Cyberspace Operations (OCO – operazioni offensive in ambito cyber). In questi ultimi mesi, alla luce della rilevanza che la dimensione cyber dei conflitti sta assumendo a livello globale, il Segretario alla Difesa Ashton Carter sta seriamente valutando l'opportunità di elevare USCYBERCOM al grado di comando combattente. Questa variazione sancirebbe, nei fatti, il riconoscimento di ciò che già avviene in realtà, ovvero che le unità cyber delle Forze Armate americane non si limitano alla sola protezione in chiave difensiva dei network militari, ma sono a tutti gli effetti anche uno strumento di attacco in tutto e per tutto simile alle unità operative nei tradizionali domini terrestre, marittimo e aerospaziale. Proprio allo scopo di continuare ad aumentare le capacità americane nel settore, il budget della Difesa statunitense per l'anno fiscale 2016 prevede che lo USCYBERCOM raggiunga i 6.000 effettivi per un totale di 133 teams operativi nelle Forze Armate. Inoltre, per il 2017, è stato presentato un budget della Difesa che prevede stanziamenti per il comparto cyber pari a 7 miliardi di dollari per migliorare ulteriormente le capacità di resilienza e l'addestramento del personale.

Da ultimo, per quanto concerne le operazioni di spionaggio di segnali elettromagnetici (SIGINT), queste sono assegnate alla NSA che ha il compito, a livello federale, di monitorare, collezionare, processare informazioni e dati al fine di soddisfare le esigenze nazionali in materia di intelligence e contro-intelligence.

CONCLUSIONI E PROSPETTIVE NAZIONALI

Da quanto fin qui esposto, si evince come la dinamica dell'adeguamento delle infrastrutture di cybersecurity e cyberdefence ad un contesto sempre più sfidante come quello attuale sia centrale in tutti i principali Paesi partner dell'Italia. Se si va, però, a confrontare le scelte organizzative straniere con quelle italiane derivanti dall'architettura del DPCM 24 gennaio 2013, tutt'ora vigente, si nota come all'estero sia prevalente una visione di "comprehensive approach" di derivazione chiaramente ispirata al mondo della Sicurezza e Difesa.

Infatti, si sta passando da un contesto di collaborazione tra diversi dicasteri, rispettando le tradizionali competenze funzionali, all'individuazione di un'autorità centrale responsabile della cybersecurity che si avvale della collaborazione di altri soggetti istituzionali in ambiti specifici. Tale entità in tutti i casi presentati è fortemente collegata al mondo dell'intelligence o della sicurezza interna (GCHQ, ANSSI, BSI, DHS e NSA) viste le possibili enormi ripercussioni in termini di sicurezza politica, economica e militare di incidenti cyber di rilievo. Potrebbe essere quindi giunto il momento, anche per il nostro Paese, di riconsiderare la scelta di affidare al MISE il ruolo di autorità nazionale di regolamentazione in materia di sicurezza e integrità delle reti di comunicazione elettronica e di interfaccia internazionale in questo settore. Un'ipotesi alternativa, analoga a quelle in fase di sviluppo presso i nostri alleati, potrebbe essere quella della creazione di un terzo servizio di Intelligence e Sicurezza Cibernetica alle dipendenze del DIS che, ferme restando le attuali competenze di AISE, AISI e del RIS Difesa in materia di SIGINT, sia effettivamente responsabile della sicurezza e dell'integrità dell'infrastruttura cibernetica del Paese. Questa nuova entità avrebbe come scopo primario assicurare innanzitutto la sicurezza della rete informatica, dei software e dell'hardware in uso da parte delle varie articolazioni dello Stato e poi, in partnership con le realtà private, delle infrastrutture critiche nazionali e della supply-chain legata alla Difesa[2]. Inoltre, tale nuovo organismo dovrebbe essere in grado, attraverso il DIS, di informare il Nucleo per la Sicurezza Cibernetica (NSC) in caso di evento cibernetico rilevante per attivare la risposta nazionale. Un terzo servizio così strutturato darebbe maggiore centralità alla necessità di protezione delle infrastrutture critiche istituzionali e civili da minacce che sono sempre più sofisticate e organizzate secondo schemi da operazione militare. Inoltre, grazie agli strumenti tipici dell'intelligence, avrebbe anche la capacità di monitorare e contrastare, anche attivamente, operazioni di ricognizione cibernetica indicative della preparazione di

2 Secondo la Relazione sulla Politica dell'Informazione per la Sicurezza del 2015, il 48% degli attacchi di cyber spionaggio a entità private nazionali ha riguardato i settori strategici dell'Industria della Difesa (18%), delle TLC (15%), dell'Aerospazio (12%) e dell'Energia (3%).

un potenziale attacco. Da ultimo, in collaborazione con le aziende e il mondo dell'accademia potrebbe fungere da elemento catalizzatore per l'adozione di standard condivisi e best practices nella prevenzione del cyber spionaggio a fini economici.

Se questa potrebbe essere una strada da seguire per rafforzare le capacità di resilienza nazionali, diviene altrettanto fondamentale adeguare il Paese anche sul fronte della minaccia rappresentata dalle cyber armi di natura prettamente militare così come raccomandato dal Libro Bianco per la Sicurezza Internazionale e la Difesa[3] . Anche in questo settore, i nostri principali alleati stanno dichiaratamente sviluppando armi offensive in un'ottica di deterrenza contro potenziali aggressori, ben consapevoli che la sola prospettiva di difesa cibernetica non è sufficiente a scoraggiare la minaccia vista l'impossibilità di proteggere tutti i potenziali bersagli sia per ragioni tecniche che economiche. Di conseguenza, sarebbe opportuno procedere allo stesso modo, implementando nel più breve tempo possibile il Comando Operativo Cibernetico Interforze (COCI) quale struttura alle dipendenze dello Stato Maggiore della Difesa (SMD). Tale struttura, integrando anche il CERT-Difesa, avrebbe lo scopo, in collaborazione con il nuovo servizio di Intelligence e Sicurezza Cibernetica, di proteggere le infrastrutture critiche della Difesa mentre gestirebbe, in via esclusiva, lo sviluppo e l'utilizzo di cyberweapons nazionali. Infatti, a parere del Ce.S.I., la capacità di creare danni fisici attraverso l'utilizzo di sistemi d'arma cibernetici deve restare di esclusiva competenza delle Forze Armate per mantenere il sistema di pesi e contrappesi stabilito dalla nostra Costituzione.

In conclusione, appare opportuno rilevare come dalla futura disponibilità di una struttura di cybersecurity e cyberdefence adeguata, e in linea con quella dei principali alleati, passerà gran parte della capacità del nostro Paese di restare competitivo politicamente, economicamente e militarmente nello scenario mondiale da qui al 2030 quando saranno completamente evidenti gli effetti della rivoluzione basata sul concetto dell' "Internet of Things".

3 Nello specifico:
Punto 32: Centralità delle reti informatiche. Il mondo sta divenendo sempre più connesso e integrato e tale situazione porta alla possibilità di avere accesso universale alle conoscenze e all'informazione. La particolare dipendenza dell'Occidente da un sistema di reti informatiche che sia funzionante, sicuro e resiliente comporta l'affermazione di un nuovo dominio operativo, quello cibernetico, che dovrà essere presidiato e difeso. Gli effetti di attacchi cibernetici alle reti o ai servizi informatici possono essere particolarmente distruttivi per i Paesi occidentali e, se di successo, comportare effetti sulla società paragonabili a quelli di un conflitto combattuto con armi convenzionali. Punto 68: Accanto a tali capacità più tradizionali, la Difesa svilupperà, in piena armonia con la strategia nazionale sulla protezione informatica, le possibilità di difesa contro attacchi di natura cibernetica che dovessero eccedere le capacità predisposte dalle agenzie civili. Analogamente, concorrerà in modo più efficace alla tutela della libertà di accesso allo spazio e alle profondità marine. Punto 103: L'estensione dei domini d'azione a quello cibernetico e dello spazio comporta che a tali ambiti siano dedicate specifiche capacità operative difensive, al fine di preservare la sicurezza del "Sistema Paese" e di rafforzare la tenuta delle strutture politiche, economiche e sociali.